1996

Strong boxes for electronic commerce

Thomas Hardjono

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Strong boxes for electronic commerce

Abstract

As electronic commerce becomes a reality, additional services related to electronic commerce will also emerge. The current paper proposes the provision of electronic strongboxes as an integrated part of the wider electronic commerce. The strongbox concept is introduced as an electronic counterpart of physical strongboxes typically found in large traditional financial institutions, such as banks, having secure vaults or other secure physical storage. The work identifies some requirements of electronic strongboxes both from the functionality perspective and from the security point of view. A simple framework for an electronic strongbox system is also presented.

Disciplines

Physical Sciences and Mathematics

Publication Details

Hardjono T and Seberry J, Strong boxes for electronic commerce, Proceedings of the 1996 USENIX Workshop on Electronic Commerce. Oakland, California, USA, November, 1996, 135-145.

Strongboxes for Electronic Commerce

(Extended Abstract)

Thomas Hardjono[1] and Jennifer Seberry

Centre for Computer Security Research
University of Wollongong
Wollongong, NSW 2522
Australia
email: thomas/jennie@cs.uow.edu.au

Abstract

As electronic commerce becomes a reality, additional services related to electronic commerce will also emerge. The current paper proposes the provision of *electronic strongboxes* as an integrated part of the wider electronic commerce. The strongbox concept is introduced as an electronic counterpart of physical strongboxes typically found in large traditional financial institutions, such as banks, having secure vaults or other secure physical storage. The work identifies some requirements of electronic strongboxes both from the functionality perspective and from the security point of view. A simple framework for an electronic strongbox system is also presented.

Keywords: Electronic Strongboxes, Electronic Commerce, Payment Systems, Distributed Systems.

1 Introduction

Electronic commerce on the Internet has become one of the major issues in computing in the last few years. The development of the world-wide-web technology and its related browsers has transformed the idea of commerce and trading on electronic media into a reality. The vast opportunities presented by electronic commerce can be easily gauged by the amount of serious interest shown by the business sector and by researchers in the field of computing.

In the business sector the number of Internet Service Providers have increased dramatically, responding to the ever greater number of people wishing to "connect to the net". The term *network computer* has been coined to capture the duality of the nature of personal computers today, namely as a desktop computer and as a gateway to the world of the Internet.

From the computer research sector quite a number proposals have been put forward for the immediate use of the Internet as a payment media through which users can carry-out transactions and payments linked to the existing physical financial infrastructure (eg. DigiCash [1, 2], iKP [3], NetBill [4] and SET [5] to name a few). Other schemes suggest the use of electronic cash or coins to be used as a circulating currency on the Internet (eg. NetCash/NetCheque [6, 7]).

As electronic commerce becomes a major activity on the Internet (and other interconnected networks), users will demand other related services to be delivered through and by the Internet. We perceive that one such service will be the provision of *electronic strongboxes* as a counterpart to the existing physical strongboxes, typically found in large financial institutions.

In the traditional financial sector the provision of strongboxes has been in service for sometime. Customers can apply to have a private strongbox held within a bank, in which the customer can place any type and any amount of valuables, subject only to the physical characteristics of the strongbox. The bank typically has no interest in the contents of the strongbox, and it derives income from providing safe storage and access to such strongboxes. The identity of the strongbox customer and the fact of the customer having a strongbox are usually treated as

[1] The author is also at the University of Western Sydney - Macarthur, NSW 2560, Australia.

confidential by the bank.

In this paper we carry-over the notion of strongboxes from the physical reality into the digital world. We propose the introduction of electronic strongboxes on the Internet as an integrated part of the electronic commerce infrastructure. It is our belief that electronic strongboxes can play an important role for the safe keeping of important items (in their electronic representation). We identify some functional requirements of electronic strongboxes which bear some resemblance to that of electronic payment protocols (Section 3 and Section 4). In addition, we present a simple framework for an electronic strongbox system, describing some of the basic interactions among the participants of the system (Section 5). The security requirements of this system is briefly discussed in Section 6. In Section 7 some security technology considerations related to the implementation of electronic strongboxes are discussed. Some remarks and conclusions in Section 8 end the paper.

2 Lockers along the Super-Highway

In today's banking world the provision of strongboxes for customers is a common occurrence. Customers typically place important items, such as jewelry and important documents, in strongboxes. Access to the strongboxes is dependent on the bank that provides the strongbox service. Usually, a bank would require a customer to identify himself or herself before access is provided. Ideally, however, access should be provided to any person when that person reveals a key that is recognized by the bank. Hence, *anonymity* of the carrier of the key is guaranteed. With the physical strongbox storage, two general approaches are usually provided:

- Customer access to a private environment containing all the non-removable strongboxes (ie. drawers).
- Customer access only to their own removable strongbox, within a private environment (ie. actual boxes)

With the current interest among the business community in conducting trade on the Internet, the notion of an electronic version of strongboxes is an interesting and attractive one. In the electronic world, and within the context of electronic commerce, banks and other certified organizations would provide the electronic strongbox service to their customers on the Internet. Customers may apply for such a strongbox over the Internet, and payment for the service can be done using electronic cash or other electronic payment forms. The customer would then have access to their respective strongboxes over the Internet, using secure browsers which allow them to place electronic items in their strongbox. There is almost no limit to the variety of electronic items that can be stored in an electronic strongbox. Some of the typical items may include:

- Electronic coins or cash
- Electronic bank cheques
- Digital documents (eg. contracts)
- Anonymous digital certificates of ownership of physical items
- Cryptographic material to access other services

A customer may have multiple strongboxes, each at differing institutions along the electronic "superhighway". Access can be provide for 24-hours per day, and the customer would be able to move items among her or his own collection of strongboxes, or two customers can exchange items that will be stored in their respective strongboxes.

Similar to the physical world, in the electronic world access can be delegated by a customer to another person by way of the customer giving the access key (or its suitable derivative) to that person. In such circumstances, the person carrying the key can access the corresponding strongbox while remaining anonymous to the institution.

A third party maybe appointed for such cases when disputes occur between an owner of a strongbox and the institution that maintains the strongbox. This may occur, for example, when a dishonest user claims that his or her access key has a matching strongbox within the bank, or when the bank inapropriately denies access to a valid owner of strongbox.

Other institutions may act as *valuers* and *converters* of legal physical items where valuable items (eg. gold) are given a valuation and an electronic certificate for the item is generated. The same institution may also provide long-term safe storage for the physical items, whilst the anonymous owner uses the electronic certificate on the Internet. The certificate can then be used for personal trade or *Barter*, which is something common in everyday life. In this context,

strongboxes can play an important role in facilitating those non-monetary commerce in an untraceable manner. Legal items may also be advertised anonymously as being "For Sale" over the Internet, with the valuers and other trusted third parties being the point of contact. In effect, these strongboxes can become a type of secure "public storage" media, where individuals can disperse their electronic properties all over the Internet, with the storage management and the actual location of their physical data being transparent to the user.

The concept of anonymous storage itself is not new. The early work by Brandt *et al* [8] points to the benefits of anonymous and verifiable databases, particularly in the context of privacy against government bodies that wish to cross-correlate data belonging to individuals in society. In [8] the true identity of each individual remains unknown and the individual employed a different *pseudonym* [9] when dealing with each government body or institution. The main feature of the work was that each individual must also have the ability to verify that his or her personal details held by an institution are correct. Further related work has also been reported in [10].

However, one underlying difference between the anonymous/verifiable database concept and the public strongbox concept is the privacy of the data. In the anonymous/verifiable database, it is intended that the institution that maintains the database view the data belonging to the users, whilst at the same time maintaining the anonymity of the users. The users can the verify that the database contains correct data about the user. A typical example would be a hospital database containing sensitive medical data belonging to patients. A patient may have personal details that are important for medical requirements (eg. blood type, diabetes, etc), but at the same time the anonymity of the patient must be upheld to prevent discrimination against some patients with serious illness (eg. cancer, HIV, etc) that could affect their entitlements (eg. health insurance, medical benefits, etc) and affect their social standing. In contrast, in the electronic strongbox concept the contents of the strongbox must remain private, with the users still remaining anonymous and being able to verify and modify (insert/remove) the contents of his or her strongbox at anytime.

In general, electronic items stored in a strongbox should be enciphered individually by its owner before they are placed in the strongbox. This approach would then allow strongbox access to be implemented in two ways:

- The owner is given the entire strongbox which she or he must open using the key, after which he or she may obtain individual items (which must be deciphered).
- The owner "delegates" the institution to open his or her strongbox and to deliver to the owner specific (encrypted) items. The institution remains unable to view the specific item requested, as the items are enciphered by the owner.

3 Functional Requirements

There are a number of basic requirements which must be fulfilled by electronic strongboxes, following the requirements of their physical counterpart. These are listed and briefly discussed in the following.

3.1 Anonymity

A1 *Anonymity of owner.*
The owner must always remain anonymous, and the fact that she or he owns a strongbox must also remain a private fact. Methods to create pseudonyms exist in other forms of electronic commerce which can be used in the strongbox case.

A2 *Anonymity of key holder.*
The key holder is the user that presents a valid key to the bank to access a strongbox held by the bank. The bank has the right to verify that the key fits into one of its strongboxes, and to deny access if the verification fails. The key holder can be the owner of the strongbox or any other user delegated to access the strongbox by its owner.

3.2 Privacy

P1 *Privacy of strongbox contents.*
As in the case of physical strongboxes, the contents of the strongbox should remain undisclosed to all parties except the key holder opening it using a valid key. Any system implementing the strongbox should ensure that the institution providing the service does not have backdoor or other hidden channels to access or view the contents of the electronic strongbox.

In addition, the strongbox should be tamper-resistant from the institution itself, who might attempt to illegally remove or add items to the strongbox. This may be achieved using cryptographic techniques (eg. hashing, signing) to provide the owner with proof and assurance that the strongbox has not been tampered with since it was last accessed.

In the physical world, some level of trust exists between the bank and strongbox owner, whereby the owner relies on the bank not to place hidden cameras designed to view the strongbox contents and that the bank will not tamper with the strongbox. Ideally, such trust should also exist between a customer and the strongbox provider, similar to the level of trust between merchant and acquirer [3, 5].

P2 *Privacy of strongbox locations.*
A user may have multiple strongboxes scattered all over the Internet under different guarding institutions. The locations of these strongboxes should be private information, available only to the owner (or any other delegated user) and the respective institutions. One institution should not be aware that its customer also owns strongboxes elsewhere.

P3 *Access to strongbox only by a key holder.*
The institution must without exception provide access to the strongbox only to the key holder that presents a valid key.

A security mechanism must be employed to provide at least two levels of verification, namely at the point of request for access to the strongbox, and later at the point of the opening strongboxes. These two levels can be implemented cryptographically, and should eliminate possibilities of procedural errors.

P4 *Storage of a variety of electronic items.*
An electronic strongbox should be able to store a variety of digital items, subject only to the agreed storage space limitations. Even such limitations should be easily and immediately negotiable when a user reaches his or her storage limit.

System parameters that protect the strongboxes must be maintained under secure and tamper-free storage at the institution.

3.3 Contents Transferability

C1 *Items exchangeable between strongboxes.*
Analogous to the physical counterpart, electronic strongboxes must allow for the exchange of items between two (or more) strongboxes. Strongboxes may belong to the same owner, or they may belong to different owners who are working together.

C2 *Untraceability of moved items.*
Since the contents of strongboxes must remain private, moved items must then be untraceable. Untraceability should hold regardless of how many times an item has been moved between strongboxes, and regardless whether or not the item finds its way into a strongbox within which it previously resided. That is, a strongbox should not have a "memory" of its previous contents.

3.4 Delegations

D1 *Strongbox key can be delegated.*
Similar to the physical strongboxes, any person carrying the appropriate key must be able to open the electronic strongbox. Ideally strongboxes should even allow stolen keys to be used, as the issue of protecting keys is separate from user anonymity.

In the banking sector some banks do provided the owner with some protection against stolen keys. However, methods that require user identification can also result in the user's identity being revealed.

In electronic strongboxes, delegation should be provided, whereby an owner of the strongbox can delegate another user to become a key holder in order to access the owner's strongbox. Both users must remain anonymous. At the same time, delegation schemes must have a limited lifetime or the ability to be revoked by the owner [11].

Single-use keys may provide a solution, in which delegated keys are derived from the original key, and where the bank holding the strongbox are aware of a key being a derivative, and would allow only one-off access to a given strongbox. Multiple-use keys may also be devised, using technology similar to electronic coins. Every usage of the key would reduce its worthiness, until it is diminished when it reaches its maximum number of usages.

4 Additional Functional Requirements

The flexibility of the digital world presents a number of opportunities to provide features of electronic strongboxes which are infeasible or difficult to achieve in the physical world.

4.1 Movable strongboxes

Electronic strongboxes should be be movable between institutions, similar to the way electronic cash or coins are movable around the Internet. An owner of a strongbox must be able either to move the entire strongbox without opening it, or to shift the contents of one strongbox at one institution to another strongbox under a different institution. Both alternatives are attractive, and both should be available to the user, depending on the user's circumstances. Security, privacy and anonymity must be ensured in both cases.

4.2 Notification to the owner

Although the owner of a strongbox must remain anonymous through the use of pseudonyms, they must be available for notifications via their pseudonym. Notifications may include:

- Notification (confirmation) that the owner's strongbox was accessed at a particular date and time (or a failed attempt was made to access the strongbox).
- Notification of fees that are due to be paid by an owner of a strongbox

4.3 Electronic charges

Owners of strongboxes pay their fees using electronic currency. This can be done on a periodic basis, or long-term payments can be made upon the commencement of the strongbox.

When an owner is absent from the Internet for a long period or when the owner fails to answer notifications concerning overdue fees, the institution may take the strongbox off-line and keep it on secondary storage (eg. dump into CD-ROM). When the owner in future requests access to the owner's strongbox, the institution can bring the strongbox on-line only after the due fees are paid by the owner. Proving ownership can be through the access key in the usual manner. Disputes with regards to payments must be resolved through a third party acceptable to the owner and the institution.

4.4 Designation of heir

An owner of a strongbox should be able to designate another valid pseudonym as an heir to be notified and given access in the case that the owner dies or the strongbox is never accessed over a long period of time (eg. years). This should occur if no prior arrangement was made by the owner with the institution regarding very infrequent access, and if the owner fails to respond to the various notifications about fees that are due. Other procedures must also be applied in the case that the designated heir fails to respond. In all these cases, the presence of a third party such as a lawyer or notary would be required as in the usual case.

The issue of property inheritance in the electronic world remains an interesting open problem, both from the legal aspect and from the economic aspect (eg. taxation in certain countries) [12].

5 A Simple Framework for a Strongbox System

In this section we propose a simple framework for a strongbox system (Figure 1), using components (ie. participants) typically found in electronic commerce systems. All electronic interactions between participants are assumed to be over a secure channel, with peer authentication conducted at the commencement of communications. The current proposal does not pretend to be comprehensive, and it attempts to address the main components only. Additional components will be required to support the framework to achieve full workability.

The participants of the system are as follows:

- *Customer*: the customer or user, interacting with the Strongbox Provider (eg. Bank) for the safekeeping of electronic items.
- *Strongbox Provider*: an institution that provides the electronic strongbox service to a customer.
- *Valuer*: the on-line Valuer is trusted to verify that an electronic item belonging to an owner

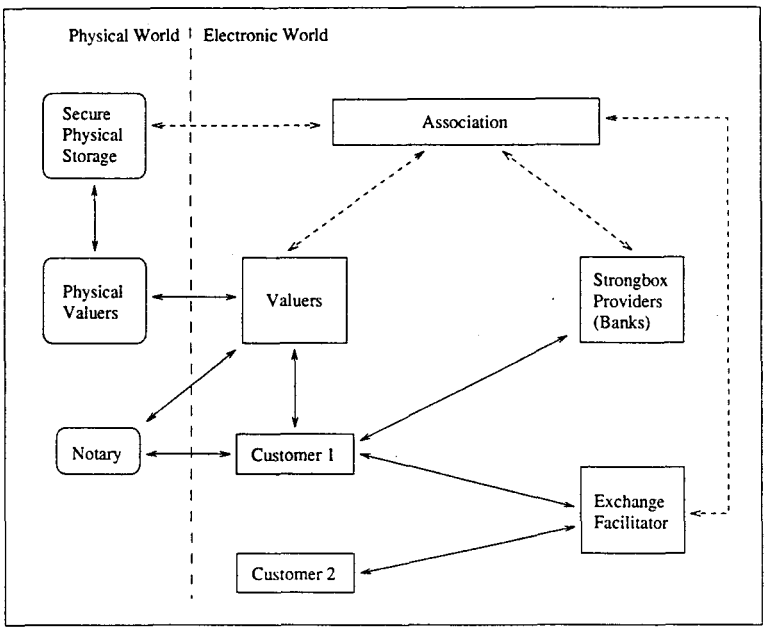

Figure 1: Electronic strongbox system

(ie. Customer) truly exists and has not been modified by its current owner. The Valuer can also be requested to split items into several sub-items, and issue certificates for them. Several Valuers may exist on-line, and each must recognize the other's certification.

- *Exchange Facilitator*: the Exchange Facilitator aids two or more Customers who wish to exchange items from their strongboxes. The Facilitator can be a Strongbox Provider and is under the jurisdiction of the Association.
- *Association*: the Strongbox Providers and the Valuer work under the umbrella of the Association. Customers bring disputes to the Association.

In addition, there are the *Physical Valuer* and the *Notary* which are in the physical world and interfaced to the electronic world. The Physical Valuer should be distinct from the on-line Valuer as the Physical Valuer knows what a physical item constitutes and which pseudonym forwarded the physical item to be valued. The Physical Valuer stores the physical items at the *Secure Physical Storage*, to which the Association has access in the case of disputes. The Notary comes in on behalf of a Customer when disputes necessitates their presence. In the remainder of this paper, unless otherwise stated, the term "Valuer" will refer to the on-line Valuer (as opposed to the Physical Valuer).

The Customer is the owner of the contents of a strongbox and is deemed also as the owner of the strongbox. The Customer obtains membership into the system through the Association which issues the Customer with the credentials (eg. within a smartcard) and with a pseudonym to be used within the system. The Customer henceforth employs this pseudonym when using the system. The Association may in fact be that which exists in the electronic commerce infrastructure and which oversees the usual electronic trading, purchases and payment. The Customer joins the strongbox service by opening an account with the Strongbox Provider, which can be a Bank or other institutions having the necessary computer infrastructure to provide this service.

In order to bring an item into the system the Customer must first obtain a valuation of the physical item to the Physical Valuer. The Physical Valuer issues the Customer with a digital certificate corresponding to the physical item. This certificate is recognized and accepted by all participants in the system. If requested, the Physical Valuer may attach a monetary value to each item, which may then be described in the certificate. The actual physical item itself is kept in the Secure Physical Storage, under the control of the Physical Valuer and/or the Association. Any Customer presenting an electronic certificate for a physical item can obtain the item from the Physical Valuer or through the Association.

The unit of the physical item to be valued and certified must be agreed upon between the Customer and the Physical Valuer (eg. six bars of gold can be written under one certificate, or six certificates can be produced corresponding to the six physical items). Having small units for the valuation allows for easier usage of the items at a later date. However, should a Customer wish to break-up an electronic item into several reasonable components – bearing in mind the physical reality of the item – the Customer can approach the on-line Valuer to obtain such services.

Here, although ideally any physical item should be allowed to be introduced into circulation, social/economic stability and order demands that illegal items (eg. drugs) be prevented from entering the electronic system. This prevention can be conducted at the Physical Valuer interface.

It remains an interesting and open problem as to whether a Customer must prove ownership of legal items. The extent to which electronic strongboxes should mimic physical strongboxes, particularly in the case of stolen goods, must be decided by authorities implementing the system.

Once within the system the certificate is referred to as an electronic item. What the item constitutes and who holds the item presently must remain confidential. A Customer can store the electronic item with any Strongbox Provider, assuming he or she already has a strongbox account with them.

When two or more Customers have agreed to exchange items, they can carry-out the exchange of the corresponding electronic items through the Exchange Facilitator. Ideally, before an exchange occurs, the Customers should prove the possession of the items to each other (eg. via zero-knowledge protocols). However, even without such pre-exchange confirmation of possession, the Exchange Facilitator must be able to ensure that no cheating occurs. The Facilitator must inform each Customer as to the electronic items it has received for the exchange instance (to prevent cheating), and the Facilitator must also provide a guarantee of non-repudiation should one (or both) Customer dispute the exchange. The Facilitator can be a trusted third party, or it can be one of the Strongbox Providers selected by both Customers.

The use of the Exchange Facilitator is optional. Customers can perform any exchange of items directly among themselves, through a secure channel. However, without the Exchange Facilitator disputes cannot be resolved and the burden of risks lie fully with the Customers.

6 Security Requirements for the Strongbox System

Similar to electronic payment systems, a number of security requirements exist for the strongbox system to be reliable and workable. It goes without saying that the *authentication* of participants holds an important place before any interaction can occur. The *impossibility of forging* of electronic items must be guaranteed throughout the system. Finally, the requirement of *undeniability of actions* (or non-repudiation) carried-out by participants in the system. Some of the other more specific requirements are briefly presented in the following.

Strongbox Provider Requirements

- *Proof of the retrieval of a strongbox.* The Provider must have some form of proof that a strongbox is currently being "checked-out". That is, that the strongbox has been retrieved and is currently in the possession of the Customer. This is to prevent the Customer from claiming otherwise and therefore forcing the Provider to take account of losses. This notion is similar to that of the forging of electronic cash or coins, or to that of denying that payments have or have not been made.

  The retrieve and store operations must exhibit the typical transaction properties of atomicity, consistency, isolation and durability [13, 14].

  A further aspect that must be taken into consideration is the allowable length of time for a strongbox to be held (checked-out) by its owner and the implications on security. Given that a Customer typically knows the contents of his or her strongbox – either from human memory or through a list stored securely (eg. within a smartcard) – it is reasonable to assume that the check-out and check-in should occur within the span of a single transaction. A reasonable timespan would similar to that in which a merchant expects immediate payment from a purchaser.

- *Verification of access key of the strongbox.* Before providing a key holder with access to the claimed strongbox, the Provider must have sufficient proof that the requester (ie. owner

or their delegate) is a valid party within the system. That is, the requester has a valid pseudonym and can be authenticated. The Provider must also verify that the key is a recognized and valid key.

One potential problem would be the possibility of the illegal duplication of access information. That is, the potential that more than one access key exists at any time. Current technology can solve this problem either through smartcard systems or through the provision of a single-use access keys for the strongboxes. In the later case, a new access key needs to be generated each time a strongbox is retrieved and stored.

Customer Requirements

- *Unauthorized retrieval of strongbox is impossible.* A Customer must have the assurance that the unauthorized checking-out of his or her strongbox is impossible. Stolen electronic items should be prevented from circulating without being detected.

  Depending on the implementation, the certificate corresponding to the item may carry the pseudonym of its current owner (see the next Section). Since the certificate is unforgeably signed by the Valuer, stolen electronic items may be detected later at an Exchange Facilitator, a Valuer or at a Physical Valuer. A possible safe-guard can be implemented at the physical end, when Customers convert their electronic items back into physical items currently being stored in the secure physical storage.

- *Proof of storage by the Provider.* A Customer requires some proof in the form of a *receipt* that his or her strongbox has been correctly checked-in and that the Provider now holds the strongbox.

- *Proof of valuation.* When an electronic item undergoes valuation or when it is split by the Valuer into several electronic sub-items, a Customer owning the item (and thus the sub-items) requires proof that the Valuer currently holds the item, and also proof that the valuation has been carried-out. Clearly the Valuer itself must be a certified one and be authenticated by the Customer before any valuation transactions occur.

- *Proof of exchange transaction.* When a Customer carries-out an exchange of items with another Customer via the Exchange Facilitator, both Customers must have sufficient proof that the exchange occurred correctly in such a way that neither party can deny the transaction.

Valuer Requirements

- *Proof that valued item and valuation result has been received by Customer.* This is to prevent a Customer accusing the on-line Valuer of stealing an item submitted for valuation.

Exchange Facilitator Requirements

- *Proof of exchange transaction.* Corresponding to the proofs required by a Customer for the exchange of an item, the Facilitator requires proof of the submission of the items to be exchanged, and more importantly proof of the delivery and receipt of the items after the exchange. This proof must come from all involved Customers, and serves as protection for the Facilitator against false claims by the Customers.

7 Technological Issues for Strongboxes

There are a vast number of issues related to the concept of electronic strongboxes and their implementation. It is beyond the scope of this introductory paper to cover each of them. Some of these, however, are briefly discussed in the following.

7.1 Representation of Electronic Items

There are many ways to represent items electronically. One possible method would be to employ two types of certificates for each item:

- *Item Certificate*: this is the electronic item itself in the shape of an unforgeable certificate and having a one-to-one correspondence with the physical item. The Item Certificate carries the signature of the Physical Valuer and is co-signed by an on-line Valuer.

- *Description Certificate*: this is a certificate guaranteeing that a given item exists somewhere in the system. The certificate may con-

tain a digest or hash of the Item Certificate, and is signed by the on-line Valuer. The certificate may contain the pseudonym of the current owner.

The two certificates are inseparable and should be stored together in the strongboxes. The aim of having a Description Certificate is to allow one Customer to prove its ownership to another Customer before an exchange occurs. During an exchange, both certificates are handed-over as an item unit.

The concept is derived from the idea of certified photocopies of important documents (eg. passports) which are often required for government and legal purposes. Periodically the Description Certificate must be renewed by way of the Item Certificate being reconfirmed by the on-line Valuer.

Similar to electronic cash, some form of serial numbering may be applied to all electronic items systemwide, to prevent illegal copying of certified items by its current owner. This must be done with the precaution that the serial numbers do not become way to trace the movement of items [15].

Upon an exchange between two Customers the Exchange Facilitator may request an on-line Valuer to re-certify electronic items as belonging to their new owners respectively. For each electronic item, both the Item Certificate and the Description Certificate must be signed by the on-line Valuer. The Description Certificate will then contain the pseudonym of the new owner of the corresponding item.

Note that no identity information, such as the pseudonym, is mentioned anywhere within the Item Certificate. Thus, the current owner of the Item Certificate may at any time obtain the actual physical item by presenting the Item Certificate to the Physical Valuer. The Physical Valuer must then inform the on-line Valuer of the removal of the item (via its serial number) from circulation within the electronic world.

7.2 Security on the User's Side

Security – or the lack of it – is currently one of the main obstacles to achieving the full use of electronic commerce on the Internet. Large financial institutions such Banks have the necessary resources to establish a reasonable level of security for their computing systems. However, security on the user's side is lacking. The vision of millions of users on their workstations or Home PCs conducting electronic commerce or trade must first address the need of trusted computing technologies at the user's end.

There a number of potential approaches that can be taken to provide security at the user's end:

- Tamper-resistant technology. Tamper-resistant boxes can be provided as part of the internal hardware for the typical PC or Network Computer (NC). Smartcards can then be used to load specific security parameters to such boxes. The challenge in the future lies in making these affordable.

- Access terminals. Institutions can provide access terminals in the manner of Automatic Teller Machines. Besides providing physical security, such terminals can be available at the institution's premises. Although practical, this approach somewhat defeats the convenience of conducting electronic commerce from the user's desktop.

- Probe software. Although a contentious issue, the notion of down-loadable self-executing software is an attractive one. Here, an institution or a trusted third party can provide auto-executables which can be down-loaded (eg. via a browser) and which can perform automatic remote scanning or probing of a user's workstation or PC/NC to evaluate its security. This notion can be extended to situations where the software reboots the workstation and loads a specific secure operating system for the workstation. After the session, the previous local operating system can be reloaded. How this concept and its implementation can be extended over wide networks – and how acceptable it will be to the user community from the privacy perspective – remains to be seen.

7.3 Multilevel Secure Strongboxes

The idea of multiple strongbox providers lends immediately to the notion that strongboxes can have differing levels of security and therefore cost of maintaining them. The frequency of access also plays an influence on the costs of the strongboxes. User's with less valuable items may choose cheaper and "weaker" strongboxes, while for their expensive items they may choose the strongest strongboxes from the variety of strongbox Providers. Each strongbox Provider may offer either a uniform

strongbox type or provide differing levels of strongboxes.

8 Remarks and Conclusion

Having proposed electronic strongboxes as part of the electronic commerce infrastructure, this paper has attempted to identify some the functional and security requirements of electronic strongboxes. This effort does not pretend to be comprehensive, as there are a number of issues that remain to be resolved in the wider context of electronic commerce, and also within the specific scope of electronic strongboxes. It also does not ignore the fact that difficulties exist in any design and implementation of the concept. We believe, however, that the concept should be tied closely to developments in electronic commerce and payment systems, as these areas will represent the infrastructure within which the electronic strongbox concept can be comfortably implemented. The current paper has presented a simple framework for an electronic strongbox system, taking the more familiar participants from electronic payment systems.

The provision of electronic strongboxes as a service should not be too far in the future, as the security technology to implement it has partly arrived accompanying electronic commerce. There are a variety of issues which must be addressed to realize strongboxes in the wider context of electronic commerce. Some of these issue include, but not limited to:

- Anonymity of Customers, while providing the various features of electronic strongboxes.
- Interfacing electronic strongboxes with physical strongboxes at the Secure Physical Storage component.
- Value of items versus strongbox costs.
- Key escrowing of strongbox-keys by governments in some countries.
- Legal status of strongboxes when the owners are foreign nationals.
- Transferability of strongboxes across national boundaries.
- Item exchanges over national boundaries and the type of Exchange Facilitators that will thus be needed.
- Effects of converting electronic items back into physical items when the new owners are foreign citizens and its legal implications.
- Valuer infrastructure required for an international strongbox system.

These issues will be the subject for continuing research as they are important for the economic viability and technical feasibility of the electronic strongbox concept.

Acknowledgements

We thank the anonymous referees for their useful comments and advice.

References

[1] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[2] D. Chaum, "Achieving electronic privacy," *Scientific American*, pp. 96–101, August 1992.

[3] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, and M. Waidner, "iKP – a family of secure electronic payment protocols," in *Proceedings of the First USENIX Workshop on Electronic Commerce*, (New York), USENIX, 1995.

[4] M. Sirbu and J. D. Tygar, "NetBill: An internet commerce system optimized for network-delivered services," *IEEE Personal Communications*, pp. 34–39, August 1995.

[5] Visa and MasterCard, "Secure Electronic Transaction," 1995. `http://www.visa.com`.

[6] B. C. Neuman and G. Medvinsky, "Requirements for network payment: The NetCheque perspective," in *Proceedings of IEEE Compcon'95*, (San Francisco), IEEE, 1995.

[7] G. Medvinsky and B. C. Neuman, "NetCash: A design for practical electronic currency on the internet," in *Proceedings of the First ACM Conference on Computer and Communications Security*, ACM, November 1993.

[8] J. Brandt, I. B. Damgard, and P. Landrock, "Anonymous and verifiable registration

in databases," in *Advances in Cryptology - Proceedings EUROCRYPT '88 (Lecture Notes in Computer Science No. 330)* (C. G. Gunther, ed.), pp. 167–176, Springer-Verlag, 1988.

[9] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[10] T. Hardjono and J. Seberry, "Applications of smartcards for anonymous and verifiable databases," *Computers & Security*, vol. 14, no. 5, pp. 465–472, 1995.

[11] M. Abadi, M. Burrows, C. Kaufman, and B. Lampson, "Authentication and delegation with smart-cards," Technical Report 67, Digital Systems Research Center, October 1990.

[12] R. Kalakota and A. B. Whinston, *Frontiers of Electronic Commerce*. Addison-Wesley, 1996.

[13] L. J. Camp, M. Sirbu, and J. D. Tygar, "Token and notational money in electronic commerce," in *Proceedings of the First USENIX Workshop on Electronic Commerce*, (New York), USENIX, 1995.

[14] L. Tang, "Verifiable transaction atomicity for electronic payment protocols," in *Proceedings of 1996 IEEE ICDCS16 International Conference on Distributed Computing System*, IEEE, May 1996.

[15] D. Chaum, "Privacy protected payments: Unconditional payer and/or payee untraceability," in *Smart Card 2000: The Future of IC Cards* (D. Chaum and I. Schaümuller-Bichl, eds.), pp. 69–93, Amsterdam: North-Holland, 1989.